

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A user authentication system, comprising:

a data holding medium for holding a common key unique to a user, used in a common-key encryption method,

wherein the data holding medium includes a radio function for sending information read from the data holding medium by radio, and writing information to the data holding medium by radio;

an authentication apparatus for holding the common key used in the common-key encryption method and a private key used in a public-key encryption method, each unique to the user; and

an information processing apparatus connected to the authentication apparatus in an always-communicable manner and provided with a function for ~~to~~ performing authentication by the public-key encryption method;

wherein the authentication apparatus performs authentication by using the common key held by the data holding medium and the common key held by the authentication apparatus, in response to a user authentication request sent from the information processing apparatus, and, only when the user has been authenticated, performs processing for making the information processing apparatus authenticate the user by using the private key corresponding to the user.

Claim 2 (original): An authentication system as claimed in Claim 1, wherein the data holding medium is portable.

Claim 3 (original): An authentication system as claimed in Claim 1, wherein the information processing apparatus is a mobile communication apparatus.

Claim 4 (original): An authentication system as claimed in Claim 1, wherein the data holding medium and the information processing apparatus are integrated as a unit.

Claim 5 (currently amended): A user authentication method for a user who carries a data holding apparatus for holding a common key used in a common-key encryption method, the method comprising the steps of:

reading the common key from the data holding apparatus by radio;

authenticating the user by the common-key encryption method by using the common key held by the data holding apparatus of the user in response to a user authentication request; and

performing, only when the user has been authenticated, processing for authenticating the user by a public-key encryption method.

Claim 6 (original): A user authentication method as Claimed in Claim 5, wherein the data holding medium is portable.

Claim 7 (original): A user authentication method as claimed in Claim 5, wherein the user authentication request is sent from an information processing apparatus.

Claim 8 (original): A user authentication method as claimed in Claim 7, wherein the information processing apparatus and the data holding apparatus are integrated as a unit.

Claim 9 (original): A user authentication method as claimed in Claim 7, wherein the information processing apparatus has a communication function.

Claim 10 (original): A user authentication method as claimed in Claim 5, wherein the data holding apparatus is an IC card.

Claim 11 (original): A user authentication method as claimed in Claim 9, wherein the data holding apparatus is an IC card.

Claim 12 (original): A user authentication method as claimed in Claim 11, wherein the information processing apparatus has a communication function, a browser function for accessing information on the Internet, and a reader and writer function for reading and writing the IC card.

Claim 13 (currently amended): An authentication method, comprising the steps of:
holding a common key used in a common-key encryption method and a ~~30~~ private key used in a public-key encryption method, for each user;

sending the common key and the private key read from each user by radio;

authenticating, in response to a user authentication request sent from an external information processing apparatus, the user by using the held common key for the user and a common key used in the common-key encryption method which the user has and is held by a data holding apparatus; and

performing, only when the user has been authenticated in the authentication step, processing for making the information processing apparatus authenticate the user by the public-key encryption method by using the private key corresponding to the user.

Claim 14 (currently amended): An authentication apparatus, comprising:

a holder for holding a common key used in a common-key encryption method and a private key used in a public-key encryption method, for each user;

the holder for holding the common key and the private key including a radio function for sending information read from the holder by radio, and writing information to the holder by radio; and

an authenticating device for, in response to a user authentication request sent from an external information processing apparatus, authenticating the user by using the common key for the user held by the holder and a common key used in the common-key encryption method for the user held by a data holding medium of the user, and for, only when the user has been authenticated, performing processing for making the information processing apparatus authenticate the user by the public-key encryption method by using the private key corresponding to the user.

Claim 15 (original): An authentication apparatus as claimed in Claim 14, wherein the authentication apparatus has a private key used in the public-key encryption method.

Claim 16 (original): An authentication apparatus as claimed in Claim 14, wherein the data holding medium is an IC card.

Claim 17 (original): An authentication apparatus as claimed in Claim 16, wherein the information processing apparatus has a reader and writer function for reading and writing the IC card.

Claim 18 (original): An authentication apparatus as claimed in Claim 14, wherein the data holding medium is integrated with the information processing apparatus as a unit.

Claim 19 (original): An authentication apparatus as claimed in Claim 14, wherein the information processing apparatus is a mobile communication apparatus.

Claim 20 (original): An authentication apparatus as claimed in Claim 19, wherein the information processing apparatus has a communication function, and a browser function for accessing information on the Internet.

Claim 21 (currently amended): A user authentication system, wherein a data holding medium for holding a common key unique to a user, used in a common key encryption method, comprising:

- a server for sending an authentication request to perform a service to the user; and
- an authentication apparatus comprising,

- a holding means for holding the common key used in a common-key encryption method for authentication between a data holding medium held by the user and the authentication apparatus, said holding means holding a private key used in a public-key encryption method to the authentication between the data holding medium and the server;

- the holding means including a radio function for sending information read from the holding means by radio, and writing information to the holding means by radio; and

- means for authenticating the data holding medium by using the common key for the user held by the holding means and a common key used in the common-key encryption method for the user held by the data holding medium in response to the authentication request sent from the server, said authenticating means performing a processing for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the common keys.

Claim 22 (currently amended): An authentication method between a data holding medium and a server by an authentication apparatus, said data holding medium holding a common key unique to a user, used in a common-key encryption method, wherein said authentication apparatus holds the common key and a private key used in a public-key encryption method, the authentication method comprising the steps of:

sending the common key and the private key from the data holding medium to the authentication apparatus by radio and writing information received from the authentication apparatus to the data holding medium by radio;

authenticating, in response to an authentication request sent from the server to perform a service to the user, the data holding medium by using the common key for the user held by the authentication apparatus and a common key used in the common-key encryption method held by the data holding medium; and

performing a processing for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the common keys.

Claim 23 (currently amended): An authentication apparatus, comprising:

a holding means for holding a common key used in a common-key encryption method for authentication between a data holding medium held by the user and the authentication apparatus, said holding means holding a private key used in a public-key encryption method for authentication between the data holding medium and a server;

the data holding medium including a radio function for sending information read from the data holding medium to the authentication apparatus by radio, and writing information received from the authentication apparatus to the data holding medium by radio; and

means for authenticating the data holding medium by using the common key for the user held by the holding means and a common key used in the common-key encryption method for the user held by the data holding medium in response to the authentication request sent from the server, said authenticating means performing a processing for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the common keys.